Integrated Financial Management (IFM) Program

Program Risk Management Framework

Version 2.0

December 31, 2004

National Aeronautics and Space Administration

NASA Headquarters
Washington, DC

Revision History

Version	Purpose	Date
1. Version 1	Original Baseline	Nov 6, 2000
2. Version 2	Revised Framework - Added new NASA Risk Matrix and corresponding Risk Likelihood and Consequence Criteria - Added Risk Manager Role to Roles and Responsibilities Table	December 31, 2004
3.		
4.		
5.		
6.		
7.		

Table of Contents

1. PURPOSE

The purpose of the Risk Management Framework is to establish the policy and guidance for managing risk on the Integrated Financial Management Program (IFMP). Roles and responsibilities for each level of Program/Project risk management as well as standard processes and techniques are identified. This framework was developed based on NASA Procedures and Guidelines (*NPG) 8000.4, Risk Management Procedures and Guidelines* and *NASA Procedural Requirements (NPR) 7120.5B, NASA Program and Project Management Processes and Requirements*. It will serve as the basis for developing detailed Risk Management Plans in support of the Program, each individual Project, and each Center. Supplemental to the Risk Management Framework is the Program Risk Management Plan, which identifies the process and methods used to manage Program-level risks.

2. DRIVERS

The overarching goal of IFMP is to improve the financial, physical, and human resources management processes throughout the Agency. IFMP will affect every National Aeronautical and Space Administration (NASA) employee and have a significant impact on the Agency's ability to successfully implement its strategic plans. Implementing these kinds of programs is very difficult. A strong risk management process, built on program management fundamentals, is key to maximizing the team's effectiveness, maintaining credibility, and ensuring that the program achieves NASA's objectives. The goal of the IFMP Risk Management program is to identify risks and either eliminate or mitigate their consequences in a cost-effective manner.

A risk is defined as an event, situation, or condition that may have a negative impact on IFM Program success in support of Agency and Functional drivers. Continuous Risk Management consists of performing the tasks necessary to identify, analyze, plan, track, control, and communicate Program risks. During the formulation phase, important unknowns critical to success will unfold as the project proceeds. These unknowns are often risks. The key to accommodating them is to recognize that one cannot know everything that may happen. Anticipating potential problems as early as possible and evaluating the potential impacts of alternative action is a continuous requirement throughout the project life cycle. Carefully assessing challenges inherent in any project is the first step in implementing a successful risk management program.

3. PRINCIPLES

The Risk Management Framework is grounded in the following set of principles developed as a result of assessing deterrents to effective risk management and best practices employed by software projects similar in nature to IFMP. These principles, listed in Table 1-1, provide a framework to accomplish effective risk management.

Table 1-1. Principles of Risk Management

Principle	Characteristics
Global Perspective	• View IFMP implementation within the context of the NASA IT Architecture. • Recognize both the potential value of opportunity and the potential impact of adverse effects.
Forward-Looking View	• Establish upper management commitment and direction with regard to the need and importance of risk management. • Manage program resources and activities while anticipating uncertainties.
Open Communication	• Encourage free-flowing information at and among all program levels. • Enable formal and informal communication. • Engage independent external reviews and assessments to identify additional risks and offer informed advice. • Track status and communicate the results of risk management activities.
Integrated Management	• Make risk management an integral and vital part of IFM Program and Project management. • Adapt risk management methods and tools to a project's infrastructure and culture. • Use bottoms-up and/or top-down risk identification analysis techniques, where applicable. • Develop risk-handling strategies that are commensurate with risk criticality. • Use measurements as early warning device • Formalize risk status reporting.
Continuous Process	• Sustain constant vigilance. o Identify and manage risks routinely through all phases of the program/project's life cycle, including developing mitigation strategies and contingency plans. o Evaluate risk management plan effectiveness
Teamwork	• Assign responsibilities for managing specific risks to the appropriate management level and individuals. • Provide Continuous Risk Management training. • Communicate lessons learned between projects and between implementing Centers.

4. ROLES AND RESPONSIBILITIES

Specific roles and responsibilities have been established for the IFM Program to achieve a high level of consistency in risk management quality, status reporting, review and evaluation, and control. These roles and responsibilities shall be used when developing Risk Management Plans.

Table 2-1. Roles and Responsibilities in Risk Management

Roles	Responsibilities
IFM Program Director (IFM Deputy Director serves as back-up)	• Appoint Program Risk Manager to actively manage Program risks • Identify top Program risks (nominally 5 – 10) for management and external status reporting • Review and validate Program risks identified by Program Staff, external reviews, and assessments • Delegate responsibility for individual risks to members of the Program Staff or Project Managers as appropriate • Approve mitigation strategies and contingency plans for Program risks • Approve invocation of risk contingency plans • Periodically monitor Program risk status, contingency plans, and mitigation efforts • Conduct Quarterly Risk Reviews (QRR) with each active Module Project, eGov Module, and IPO • Periodically report risk status, trend analysis, and success of mitigation efforts of Program's top risks and selected Project-level risks to the Program Management Council and external entities.
IFMP Staff	• Identify new risks (using risk identification techniques) • Report new risks to Risk Manager, Project Lead, etc., as they are identified.
Program/Project Risk Manager	• Work with the Program Director/Project Manager to review and validate Program/Project risks identified by Program/Project Staff, external reviews, and assessments • Assist Risk Owners in developing risk statements, performing risk assessment and mitigation strategies, as required • Track all Program/Project risks in a Risk Database • Work with Risk Owner to assess, monitor, and control Program/Project risks, as required • Facilitate periodic Program/Project risk reporting and status updates • Facilitate QRRs and review Project QRR briefings (Program Risk Manager) • Prepare Project QRRs (Project Risk Manager) • Report Program/Project risks via the Erasmus tool (if able to access) and MSR monthly • Review the Program/Project Risk Management Plan annually and update as required.

Roles	Responsibilities
Risk Owner	• Perform risk assessment (e.g., writing risk statement and assigning likelihood, consequence, criticality ratings, and timeframes) • Develop and implement handling options and mitigation strategies for assigned risks • Periodically report risk status, trend analysis, and success of mitigation efforts in reducing the likelihood and/or consequence of assigned risks • Document lessons learned and potential best practices
IPO, Module, and eGov Project Managers	• Develop IPO, Module, and eGov Project Risk Management Plans consistent with IFM Program Risk Management Framework • Delegate responsibility for individual risks to members of the IPO, Module, and eGov Project staff, or elevate to the Program Office level as appropriate • Identify top IPO, Module Project, and eGov Project risks (nominally 5) for management and external status reporting • Approve mitigation strategies for top Project risks • Provide monthly risk status, trend analysis, and success of mitigation efforts of IPO, Module Project, and eGov Project top risks via MSR briefings • Perform reassessment of existing risks quarterly and report during QRRs • Approve Centers' IFM Risk Management Plans
NASA Center Lead for IFMP	• Manage Module Center implementation and change management risks for NASA Center • Develop NASA Center's Risk Management Plan (shall be incorporated into Center Implementation Plan) • Review and validate implementation and change management risks identified by Center Implementation Team members, periodic external reviews, and assessments • Delegate responsibility for individual deployment and change management risks to members of the Center Implementation Team • Identify top Center implementation and change management risks for management and external status reporting, and provide to the Program Risk Manager • Approve risk mitigation strategies for top Center risks • Continuously monitor NASA Center risk status, trend analysis, success of risk mitigation efforts, and contingency plans • Provide monthly report status, trend analysis, and success of mitigation efforts and contingency plans of NASA Center's top risks to Program Risk Manager (via MSR briefing) and external entities.
External Reviewers (e.g., IFMP Steering	• Periodically review risk status, trends, and success of mitigation strategies, and contingency plans for top Program, IPO, Module,

Roles	Responsibilities
Council, Program Management Council, Center Management, NAR/IAR, Program Change Management Contractor, Program Implementation Contractor)	and eGov Project risks • Identify new Program risks • Recommend risk handling options, mitigation strategies, and contingency plans for identified risks to the Program Manager.

5. REQUIRED ELEMENTS OF RISK MANAGEMENT PLANS

IFMP Risk Management Plans should be developed based on NASA's Continuous Risk Management Model shown in Figure 2-1. Additionally, plans should address roles and responsibilities.

Figure 2-1. NASA's Continuous Risk Management Model

Required Risk Management Plan Elements

- Organization, Roles, and Responsibilities
- Risk Identification
- Risk Analysis and Prioritization
- Risk Control (Planning, Handling, Tracking)
- Communications and Reporting
- Tools and Techniques
- Risk Management Commitment and Effectiveness Measures

For each element (except organization, roles, and responsibilities), the following topics should be addressed:

- Process steps
- Participants in the process
- Inputs
- Outputs
- Tools and techniques.

5.1 RISK IDENTIFICATION

Risk identification is the first step in the risk assessment process. The purpose of identification is to consider risks before they become problems and to incorporate this information into the

program and project management process. Risk identification depends heavily on open communication and a forward-looking view to encourage all personnel to bring forward new risks. Anyone in the program can identify risks. The description of the risk should be clear, concise, and sufficiently informative that the risk is easily understood. The process by which risks are identified should address the topic areas listed in Table 2-2.

Various tools and techniques can be used to assist in risk assessment. Each Project and NASA Center should consider using a set of risk assessment tools and techniques appropriate to their implementation needs. Each project will conduct risk assessment in a structured approach and employ two different perspectives—Top-Down Approach and Bottoms-Up Approach. Appendix A describes tools and techniques that may be used to illustrate both the top down and bottoms up approaches.

Table 2-2. Risk Identification Topics

Topics	Approach
Process Steps	• How risks are identified • How and when independent review and assessment advice is incorporated • How risks are documented (e.g., using a 'condition-consequence' format, wherein a risk reads as follows: "*Given the <**condition**>, there is a possibility that <**consequence**> will occur*").
Participants	Specific role in risk identification, as applicable, for: • Program Director • Project Manager • Risk Manager • Risk Owner • NASA Center Lead • IFMP staff members • External reviewers
Inputs	Success criteria, project environment and constraints, and lessons learned. For example: • First principles • Agency and Functional drivers • Success measures and benefits • System concept of operations • Program/project constraints
Outputs	• List of approved risks • Risk Owners • Changes to risk database
Tools and Techniques	Explanation of approach and tools used for: • Top-down techniques such as lessons learned, best practices, and Fault Tree Analysis (FTA) • Bottom-ups techniques such as Failure Mode, Cause and Effect Analysis (FMCEA)

5.2 RISK ANALYSIS AND PRIORITIZATION

The purpose of risk analysis is to convert data into decision-making information. Analysis is the process of examining the risks in detail to determine the extent of the risks, how they interrelate, and which ones are the most important. Risk analysis consists of four basic activities:

- Concisely stating the risk – NASA guidance suggests that risks be written using a 'condition-consequence' format, wherein a risk reads as *"Given the <**condition**>, there is a possibility that <**consequence**> will occur."*
- Determining risk likelihood – Appendix B depicts a Risk Likelihood of Occurrence Rating tables to be used as a guideline in developing more specific characterizations of each likelihood level.
- Assessing risk consequences – Appendix C provides more information about the risk categories and Risk Consequence Rating tables to be used as guidelines in developing more specific characterizations of category consequences.
- Determining risk criticality – Using the Likelihood and Consequence ratings, a risk criticality is assigned according to the Risk Criticality Matrix in Appendix D.
- Estimating risk timeframes – There are two risk timeframes – the consequence timeframe that refers to whether the consequence of a risk is likely to occur and the mitigation timeframe that refers to timeframe within which action should be taken to mitigate the risk.
    - Near-term – Less than 90 days
    - Mid-term – 90-180 days
    - Long-term – More than 180 days.

The process by which risks are analyzed should address the topic areas listed in Table 2.3.

Table 2.3 - Risk Analysis and Prioritization Topics

Topics	Includes
Process Steps	Analysis and prioritization process to include how the project will address the following: • Consolidation of similar risks • Evaluation of risk criticality based on overall likelihood and the highest individual consequence for each risk category: Cost, Schedule, Integration/Technical, Mission Success • Prioritization risks • Identification of risk consequence and mitigation timeframes • Identification of top risks • Receipt of management approval
Participants	Specific role in analysis and prioritization activities, as applicable, for: • Program Director • Project Manager

Topics	Includes
	• Risk Manager • Risk Owner • NASA Center Lead • IFMP staff members • External reviewers
Inputs	• Documented list of approved risks
Outputs	• Prioritized List of approved risks, with associated attributes • Changes to risk database
Tools and Techniques	• Explain tools and techniques used (e.g., how likelihood is determined)

5.3 RISK PLANNING, TRACKING, AND CONTROL

The purpose of risk planning, tracking, and control is to decide what, if anything, should be done about a risk or set of related risks, to plan and take appropriate mitigation actions, and to assess the effectiveness of mitigations. The process by which risks are analyzed should address the topic areas listed in Table 2.4.

Table 2-4. Risk Planning, Tracking, and Control Topics

Topics	Includes
Process Steps	Risk planning, analysis, and control process to include how the project will address the following: • Determining handling options for each risk • Developing appropriate mitigation strategies and contingency plans • Identifying risk attribute metrics • Implementing mitigation strategies as a appropriate • Monitoring risk attributes metrics • Identifying new risks • Evaluating effectiveness of mitigation strategies • Executing contingency plans as necessary
Participants	Specific role in analysis and prioritization activities, as applicable, for: • Program Director • Project Manager • Risk Manager • Risk Owner • NASA Center Lead • IFMP staff members • External reviewers • Quality assurance
Inputs	• Prioritized list of approved risks • Risk criticality analysis
Outputs	• Risk mitigation strategies • Changes to risk databases

Topics	Includes
	• Contingency plans • Risk attribute metric • Risk management status • Risk Status via the MSR briefing
Tools and Techniques	• Explain tools and techniques used, for example, to track risks and measure mitigation effectiveness

The Program Office currently uses Erasmus to track its top 10 risks. Projects may use other tracking tools that capture the required risk information. Additionally, the Program and Projects use the Knowledge Sharing Systems to capture lessons learned (often used to identify potential risks and/or mitigation activities that were successful or unsuccessful for planning purposes.

Risk Planning. Using the Risk Criticality Assessment discussed in Section 2.3, a risk handling option is assigned to each risk. The standard IFM Program Risk Handling Options are listed below in Table 2-5:

Table 2-5. IFM Risk Handling Options

Option	Approach	Possible Criticality Rating
Transfer	Reallocate the risk to others	High, Medium, Low
Accept	Do not develop mitigation strategies; prepare written rationale and identify contingency strategy if needed	Medium, Low
Watch	Monitor risk attributes; establish metrics	Medium, Low
Mitigate	Eliminate or reduce likelihood of occurrence or consequence; identify contingency plan	High

Risk handling rules have been established by the IFM Program, and will be applied to each risk based on the risk criticality. Any variance of the Risk Handling Rules will need to be justified in the Risk Management Plan and approved by the IFM Program Director:

- All HIGH criticality risks require both a mitigation strategy and a contingency plan.
- MEDIUM criticality risks require a contingency plan. Mitigation strategies may be required.
- LOW criticality risks typically do not require a mitigation strategy or contingency plan.

Note: Medium risks do not *require* mitigation strategies because the Program may choose to accept the risk. In this instance, the Program decides that it will not expend resources to mitigate the risk and takes a chance that the risk will not be realized. However, all Projects must develop contingency plans to prepare for impacts if the risk becomes an issue.

Using these options, specific risk mitigation plans should be developed and implemented. Likewise contingency plans should be invoked when a risk has been realized, realization is inevitable and near-term, or mitigation strategy success is highly unlikely.

It is not possible or practicable to eliminate all risks. The costs incurred to eliminate or reduce risk must be weighted against the benefits. In most projects, Pareto's law applies: 20% of the individual risks represent 80% of the potential for project failure. Thus, a necessary part of risk planning includes estimating and allocating risk contingency reserves for Program and Project risks. A comprehensive methodology has been developed to facilitate this process. Appendix E provides detailed information about the contingency reserve allocation process.

Risk Tracking. Each Project or Program Risk Manager should track and manage risks using a Risk Database. This database can be any application that the Project or Program deems adequate (e.g., MS Excel spreadsheet, MS Access database, etc.). At a minimum, the risk database should track the risk statement; risk owner; likelihood, consequence and criticality ratings; risk timeframes; mitigation statements; and current status of risk activities. To enable the Program to maintain insight into top Program-level risks, each Project and NASA Center will Provide risk status via the MSR briefing. The data provided should include the minimum risk attributes outlined in the MSR template. Additionally, Projects should be sure to include change management risks.

Risk Control. Risk Control is putting the results of risk tracking into action – actually reviewing risk activities to adjust mitigation strategies and managing contingency plans. The Risk Manager and/or Risk Owner are responsible for resubmitting plans for approval and managing contingency activities. New or revised activities should again be included in the Program or Project schedule.

5.4 COMMUNICATIONS AND REPORTING

The purpose of communicating and documenting risk information is for all personnel to understand the risks and mitigation alternatives as well as the risk data to make effective choices within the constraints of the IFM Program. Communication and documentation are critical for managing risks. Referencing the Risk Communications and Reporting Diagram provided in Appendix G, each Risk Management Plan should establish:

- Specific and periodic risk management review points
- Information transfer mechanisms
- Independent reviews and assessments.

5.5 RISK MANAGEMENT COMMITMENT AND EFFECTIVENESS MEASURES

An important component of the Risk Management Plan is the identification of metrics to determine management commitment and the effectiveness of risk management procedures. This is necessary to ensure that active, diligent management continues.

To determine the level of management commitment, the effective risk management plans should reflect the following:

- Existence of formalized risk status reporting
- Formal delegation of risks to appropriate managers
- Incorporation of mitigation activities for top risks into Program/Project/Center schedules.

The following metrics can be used to help the IFM Program and Projects determine the effectiveness of individual risk management strategies, including making judgments of the effectiveness of risk handling plans and mitigation strategies in reducing the likelihood of occurrence and/or projected risk consequence:

- Number of risks identified over time (using Trend charts)
- Number of risks with active mitigation strategies (using Trend charts)
- Number of risks closed (using Trend charts)
- Changes in level of criticality for each of the top risks (using Fever chart)
- Identification of risks that have materialized and become issues
- Identification of risks that have been mitigated.

Evaluation of risk strategy effectiveness may result in revisions to the risk management plans, individual risk mitigation strategies, or re-working of risk criticality assessment matrix.

6. REFERENCES

NASA Procedures and Guidelines (NPG) 7120.5B, NASA Program and Project Management Processes and Requirements, November 21, 2002

NASA Procedures and Guidelines (NPG) 8000.4, NASA Risk Management Procedures and Guidelines, April 25, 2002

NASA Integrated Financial Management Program (IFMP) Program Management Plan, February 7, 2002

IFM Program Risk Management Framework, Version 1, November 7, 2000

IFMP Benchmarking Resource Library Framework, Version 1, September 15, 2000

Continuous Risk Management Guidebook, Software Engineering Institute at Carnegie Mellon University, 1996

California Health and Human Services Website, http://www.bestpractices.cahwnet.gov/Support%20Processes/Risk%20Mgmt/risk%20mgmt%20-%20planning.htm

Risk Management: Guidelines and Best Practices, Missouri Information Technology Advisory Board, Project Management Committee, Risk Management Subcommittee, November 2003

APPENDIX A - RISK IDENTIFICATION/ANALYSIS TOOLS AND TECHNIQUES

Effective risk identification and risk assessment is the critical first step in an effective risk management program. If risks are not identified and assessed early, they often appear later as issues that must be handled in a reactive sense, often with significant cost, schedule, and performance consequences. The IFMP risk management approach proactively identifies risks, focuses on critical elements, and develops effective strategies that, when implemented, manage risk on an equal footing according to cost, schedule, technical, and performance metrics. To ensure a comprehensive assessment of potential risk, each project should be evaluated using one or both of the following perspectives:

(1) A Top-Down assessment from a mission success perspective
(2) A Bottoms-Up assessment that concentrates on the individual contributors to risk.

Under both approaches, the specific technique employed by a project can vary significantly in terms of fidelity and structure. Every effort should be made to ensure a comprehensive and formal assessment of risk. Each Project shall review the range of potential techniques for applicability, resources and time to implement, and projected benefit during the project formulation phase.

Top-Down Assessment

Description. A top-down approach should focus on mission success and identify those attributes of the project that are necessary for success. The analysis can focus on schedule events, working from success through the start of the program, or specific functions that need to be accomplished to successfully implement the project. Initially the focus is less on how an event could happen and more on identifying events that through historical perspective or logical dependency could have significant impact on the potential for success. This then provides a basis for analyzing potential root causes, likelihood, criticality, and mitigation approaches. Often, benchmarking and lessons learned are very useful tools to facilitate the analysis. FTA is a more formal approach to defining events and providing a structure for analysis of likelihood and consequences.

Lessons Learned Libraries. IFMP has established and maintains a Knowledge Sharing System (KSS) to capture and make available lessons learned and best practices regarding detailed IFMP-specific and historical lessons learned, other NASA projects of similar size, industry best practices, and best practices that are peculiar to the IFM Program. The KSS provides the capability to disseminate pertinent information to appropriate Program and Project members in a timely manner to facilitate decision-making and identify opportunities for process improvement. This KSS and the NASA Lessons Learned database can be important information resources to help identify potential risks and successful mitigation strategies.

Fault Tree Analysis Technique. FTA is a deductive technique often used in risk/reliability analysis. FTA utilizes a hierarchical representation of dependencies in a top down approach for assessing the likely causes of a failure of a high (top) level event. A model is developed that logically and graphically represents the various combinations of possible events, activities, and components that contribute to the success or failure of a high (top) event. The fault tree does not

necessarily contain all possible points of failure. The fault tree contains only those events, activities, and components whose existence contributes to the success or failure of the top event. Significant subjectivity is used to establish the hierarchy and effects. Probabilities of success or failure can be applied to each event, activity, and component. Analysis postulates a high level (top) negative event, then descends through a hierarchical model of supporting events, activities, and components, identifying the path and extent of failures that must occur in order to cause the top event to fail. FTA helps to determine:

- Requirements and functionality most critical to the success of a functional module
- Areas where resources should be focused
- Likelihood of module success based on developing success or failure of hierarchy components
- Potential effects of functionality gap on module success
- Areas of risk requiring workarounds.

Use of this technique requires significant expertise in the following areas:

- The technique itself
- Functional areas – Concept of operations, functionality requirements
- Technical areas – Testing, interfacing, Commercial off-the-shelf (COTS) functionality.

Following is an example of how FTA might be applied to Resume Management. This technique is useful in determining the effects that gaps between COTS functionality and requirements have on defined success measures, benefits, and functional drivers.

A hierarchical Resume Management model was developed based on the Business Case Analysis. Success of the Resume Management module is dependent upon the Project's success in achieving each of the individual functional drivers. Each functional driver is supported by success measures and benefits. Success or failure of achieving a functional driver is based on the degree to which the success measures and benefits are accomplished. At the bottom of the hierarchy, requirements and functional attributes are aligned with the success measures and benefits they support. Judgments as to whether success measures are met and/or benefits are achieved depends on the specific functionality provided and requirements met by a potential COTS tool.

Judgments were made regarding the criticality of each functional driver:

- Critical functional drivers are connected by 'OR' conditions; the failure of a critical functional driver suggests failure of the functional module
- Contributing functional drivers are connected by 'AND' conditions; the failure of all functional drivers connected by 'AND' conditions suggests failure of the functional module
- Non-critical functional drivers do not contribute to the failure of the functional module and are not included in the hierarchy.

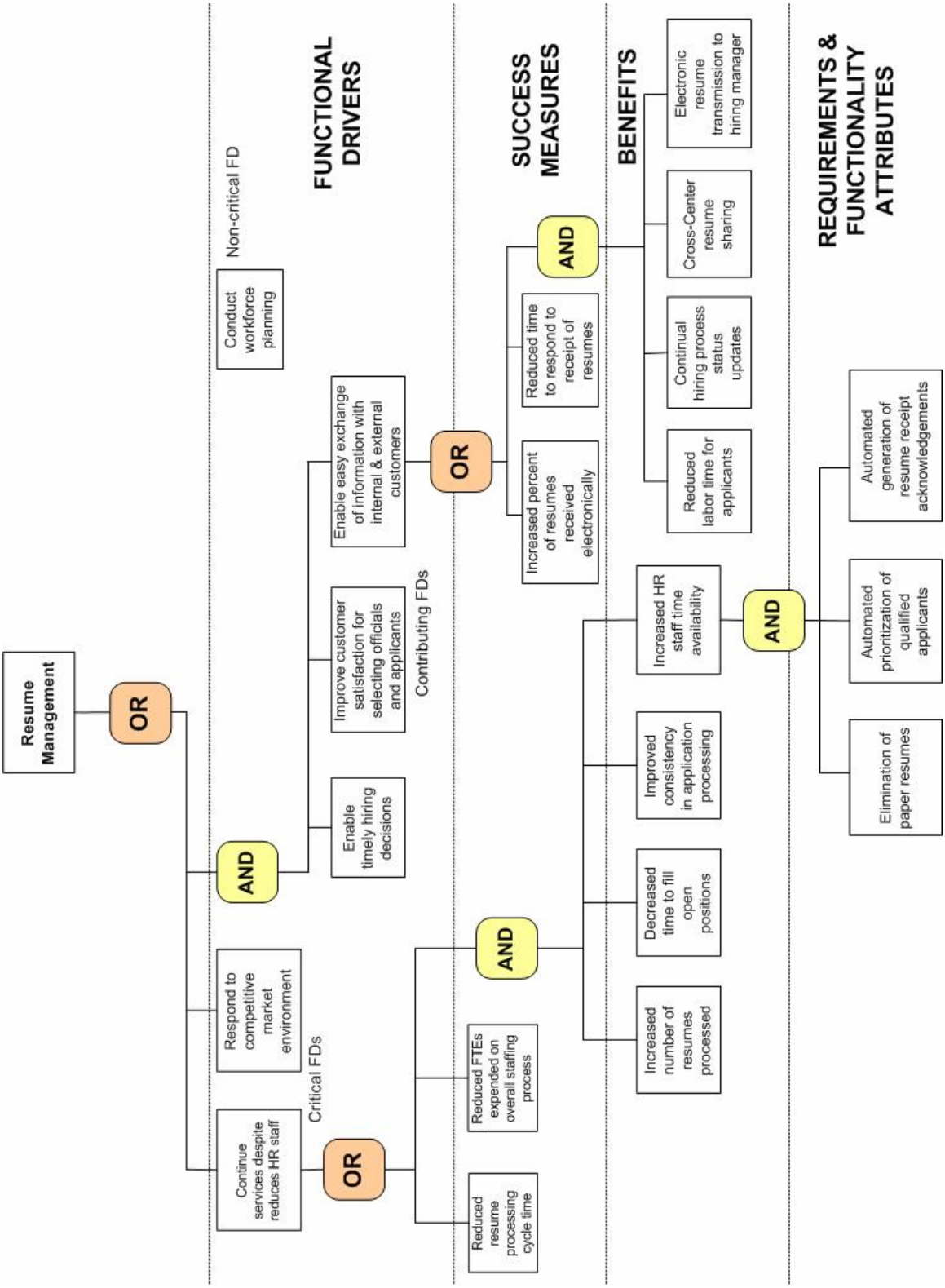
Judgments were made regarding the criticality of each success measure and benefit:

- Success measures supporting functional drivers are connected by 'OR' conditions; the failure of a success measure suggests failure of the functional driver
- Benefits supporting functional drivers are connected with 'AND' conditions; the failure of all benefits connected by 'AND' conditions suggests failure of the functional driver.

Judgments were made regarding the requirements and functional attributes contributing to the success of each success measure or benefit:

- Contributing requirements and attributes are connected with 'AND' conditions
- Failure of all contributing requirements and attributes connected by 'AND' conditions suggests failure of the associated success measure or benefit.

Figure A-1. Application of Fault Tree Analysis to Resume Management



Bottoms-Up Assessment

Description. A bottoms-up approach involves the expression of the project as a detailed set of events or activities followed by the identification and mitigation of potential causes of failure. This approach is structured around the lowest elements of the project, either in a functional work breakdown structure sense or in terms of sequence of events to reach a result. Individual risks are evaluated and then aggregated to establish collective risks to determine project vulnerability. The approach presumes there is a basis for assessing risk at the component level. In hardware projects, there is often substantial statistical data on the failure rate for individual components, assemblies, and systems. This highly quantified data is often not feasible in the IFMP-type of COTS-based administrative systems. However, it is possible to provide rough estimates of risk at this level of aggregation. For example, a sub-process in the Core Financial software that has significant gaps in functionality has higher technical risk than one where the native software code fully supports the "go to" process requirements. In a similar manner, a sub-process that is fully supported by the software but represents a significant process change has a higher change management risk. In both cases, high-risk items can be identified, their contribution to project success evaluated, and mitigation strategies developed based on the assessed failure modes and root causes. FMCEA is an example of a rigorous bottoms-up technique.

Failure Mode, Cause, and Effect Analysis (FMCEA). FMCEA is a bottoms-up inductive analysis technique used at the event, activity, or component level to define, identify, and eliminate known and/or potential failures. FMCEA lends itself to evaluating discrete events (e.g., a system test is successful or fails, a schedule control point is achieved or missed) as opposed to making a judgment as to the level of success (e.g., how well does system functionality support a requirement).

FMCEA can be used as an early warning technique that employs a systematic approach to examining potential points of failure and associated causes and effects. Each failure mode may have multiple causes and precipitate multiple effects. Failure modes can be prioritized according to impact on system success measures, benefits, and functional drivers. FMCEA analysis can help determine:

- Discrete events or components most critical to the success of the functional module
- Obvious risk mitigation strategies
- Potential effects of event or component failure
- Areas of concern where resources should be focused.

Use of this technique requires significant expertise in the following areas:

- The technique itself
- Functional areas – Concept of operations, functionality requirements
- Technical areas – Testing, interfacing, COTS functionality

Following is an example of how FMCEA was applied to Resume Management; useful in supporting the test phase, where events (tests) are either successful or they fail.

Table A-1. Resume Management FMCEA Example

Component	Failure	Cause	Effect
Import Resumes from USA Jobs	Test fails format	1. Incompatible data	Paper resumes are not eliminated
		2. Communications issues	

In this example, a system component (e.g., ability to import resumes from USA Jobs) is projected to fail during system testing. Having projected the possible causes for such a failure, risk mitigation strategies can be developed to decrease the likelihood that this risk would materialize. For example, the following risk mitigation strategies may apply:

- Compare, analyze, and test for data format compatibility prior to system testing
- Test communication, security, and file access protocols prior to system testing.

APPENDIX B – RISK LIKELIHOOD RATINGS

Each risk will be assigned a likelihood of occurrence rating based on risk likelihood table shown in Table B-1.

Table B-1. Likelihood Ratings

Rating	Likelihood of Occurrence	NPG 8000.4 Guidance
5 Very High	Event is in imminent danger of occurring and current process or approach will likely not prevent this event. Risk should be considered for transition to an issue.	Likely to occur
4 High	Event may occur and current process or approach will likely not prevent the event.	Probably will occur
3 Moderate	Event may occur but current process or approach may prevent it from occurring.	May occur
2 Low	Current process or approach is usually sufficient to prevent this type of event. The event probably will not happen.	Unlikely to occur
1 Very Low	Current process or approach is sufficient to prevent this event from occurring.	Improbable

APPENDIX C – CONSEQUENCE ASSESSMENTS

Each risk is assigned a risk consequence for each applicable risk categories. The risk categories and risk consequence rating tables are provided below. When a risk is associated with multiple risk categories, the risk's consequence in each associated category is assessed and tracked.

Cost
- Budget
- Staffing

Schedule
- Blueprinting
- Realization
- Go-Live

Integration/Technical
- System module deployment
- Integration complexities
- IT infrastructure
- Performance

Mission Success
- Agency business drivers and Integration Project functional drivers
- Functional requirements
- Gap in system functionality vs. requirements
- Successful reengineered process implementation
- Effective Program change management

The tables that follow are used to assess the consequences of each risk according to the identified risk category. When a risk is associated with multiple risk categories, the risk's consequence in each associated category is assessed and documented (tracked).

Table C-1a. Consequence Ratings for Cost Risks

If event "X" were to occur, then the cost consequences would be:

Rating	Cost Criteria
5 Very High	• Event will cause Program or Project end of year (EOY) Manager's estimate to exceed current plan by more than 15%; **or** • Total cost increase cannot be supported by existing Program funds; **or** • Negative budget event will impact Program funding available for pending modules, causing a delay in initiating new modules and/or eliminating planned modules.
4 High	• Event will cause Project Manager's EOY estimate to exceed current plan by more than 10, but less than 15%; **or** • Total cost increase cannot be supported without full use of project reserves plus additional funds from Program reserves.
3 Moderate	Event can be covered by full use of available project funding reserves and project manager believes that project can be completed without requesting additional funding.
2 Low	Event impact will be limited to task or activity and any cost overruns can be fully covered by partial use of available project reserves not to exceed 30% of remaining reserves.
1 Very Low	Event can be resolved with minor use of project reserves (less than 5% of remaining reserves).

Figure C-1b. Consequence Ratings for Schedule Risks

If event "X" were to occur, then the schedule consequences would be:

Rating	Schedule Criteria
5 Very High	Project performance related issues or decision-making delays would cause the project end date to be missed with significant impact on Program commitment or loss of executive management commitment. Project commitment date cannot be met through use of schedule reserve.
4 High	Performance related issues or decision-making delays will cause significant impacts to critical path and current project phase completion date cannot be met through use of schedule reserve. Project commitment date is not effected.
3 Moderate	Performance related issues or decision making delays will cause project milestones to be missed, but current project phase and Project end date are not jeopardized and can be achieved through use of schedule reserve.
2 Low	Performance related issues or decision making delays will cause delays to individual deliverables or task completion dates, but major milestones, project phases and project end date can be achieved on time.
1 Very Low	Performance related issues or decision making delays will not cause schedule delays that cannot be covered without use of any existing schedule reserve.

Figure C-1c. Consequence Ratings for Technical Risks

If event "X" were to occur, then the technical consequences would be:

Rating	Technical Criteria
5 Very High	Program/Project will not meet minimum mission or technical success/exit criteria and no alternatives exist.
4 High	• System performance will be unsatisfactory during periods of normal operations; **or** • System solution will be incompatible with NASA's IT standards; **or** • System will be unable to satisfactorily integrate with other systems or IFM modules.
3 Moderate	• System will experience unsatisfactory performance degradation during peak load periods; **or** • Software will not support some Agency IT standards.
2 Low	• System will experience noticeable, but acceptable performance degradation during peak periods; **or** • Software will not support some IT standards but upgrades are scheduled/expected.
1 Very Low	• No system performance degradation will occur during normal operations; **and** • - System will support IT standards.

Figure C-1d. Consequence Ratings for Mission Success Risks

If event "X" were to occur, then the mission success consequences would be:

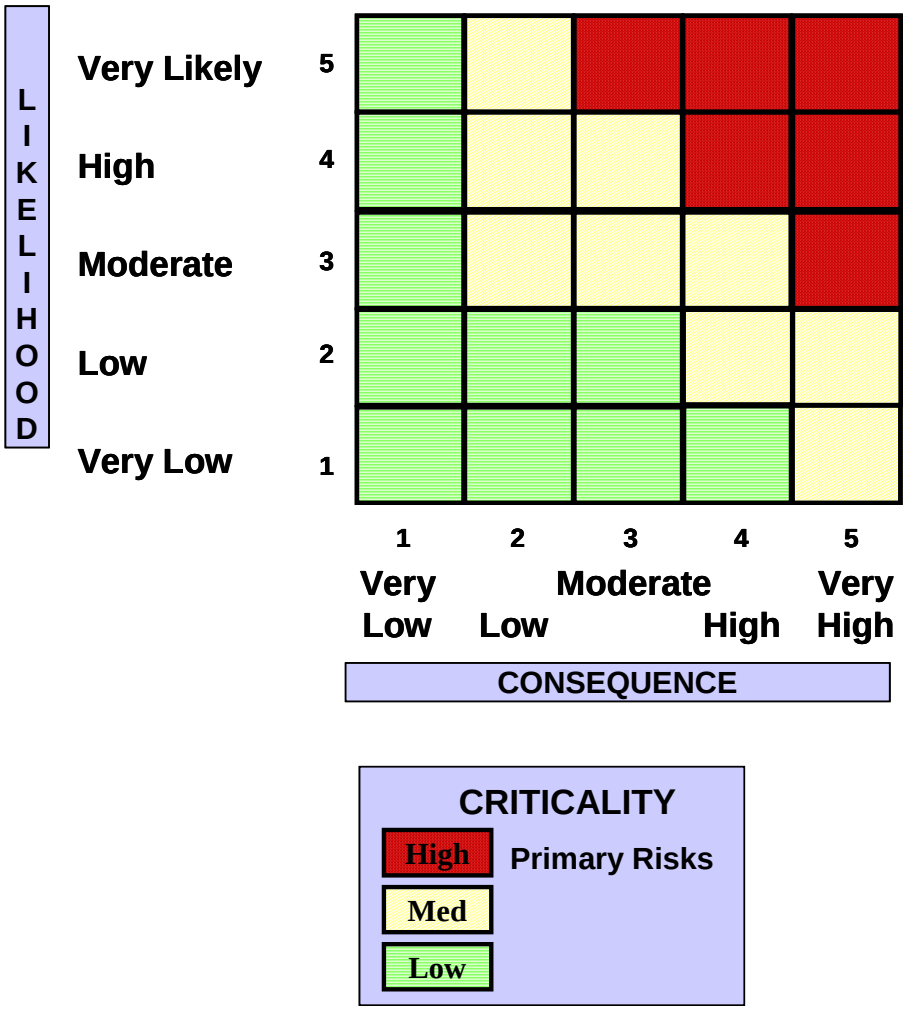
Rating	Mission Success Criteria
5 Very High	• Major functionality will be lost and gaps cannot be closed; **or** • Event will cause project to achieve less than 50% of functional driver benefits realization; **or** • System will be rejected by users and functional community.
4 High	• Major functionality will be lost but gaps can be closed by using additional software bolt-ons; **or** • Event will cause project to achieve less than 70% of functional driver benefits realization; **or** • Majority of users will reject the system and significant additional transition support is required to overcome resistance.
3 Moderate	• Significant functionality will be lost but gaps can be accommodated by process changes or workarounds; **or** • Minor additional transition support will be required to overcome user resistance; **or** • Benefits realization will be substantially below expectations for one functional driver.
2 Low	• Functionality loss will be acceptable and any gaps will be closed

Rating	Mission Success Criteria
	using future enhancements/fixes; **or** • Minor user resistance will be encountered not requiring additional transition support; **or** • All critical functional driver benefits will be met by module.
1 Very Low	• Functionality loss will be acceptable and no gap closure is necessary; **and** • Users will accept new system; **and** • All expected benefits will be achieved.

APPENDIX D - RISK CRITICALITY ASSESSMENT MATRIX

Using the Likelihood and Consequence Rating tables, each risk is assigned a likelihood and consequence rating in each of the affected risk categories. Using these ratings, a Risk Criticality Assessment Matrix is generated for each risk. The criticality is determined by plotting the likelihood and consequence ratings and then determining which area the risk falls into. The highest level of consequences among the affected categories is used to calculate risk criticality.

Figure D-1. Risk Criticality Assessment Matrix



APPENDIX E – CONTINGENCY RESERVES ALLOCATION PROCESS

As part of the annual budgetary process, reserves are to be calculated for the Program Office, the Integration Project Office, and each of the Module Project Offices. The reserves are risk-based; every dollar of reserves should be tied directly to the cost of occurrence of a specific risk.

General Concept. The procedure to calculate reserves and incorporate them into the budget is a three-tiered process. The first part consists of the respective office identifying risks and allocating a reserve dollar amount to each one of the risks. A likelihood of occurrence and a level of consequence are also identified, which together determine the criticality of the risk based on the risk matrix in Appendix D. The second step of the process is for the Program Office to collect all of the information from the various offices and to use the provided information to create frequency distributions around each of the risks. Based upon the likelihood of occurrence of each risk, confidence levels are assigned, which provide a rigorous reserve amount. In the third step the Program Office reviews the assigned reserves with each of the owners and makes any final adjustments before incorporating them into the budget. In the case that the scope or the schedule changes to the pertinent projects, this procedure must be repeated to ensure that the reserves allocation accurately reflects up-to-date risks.

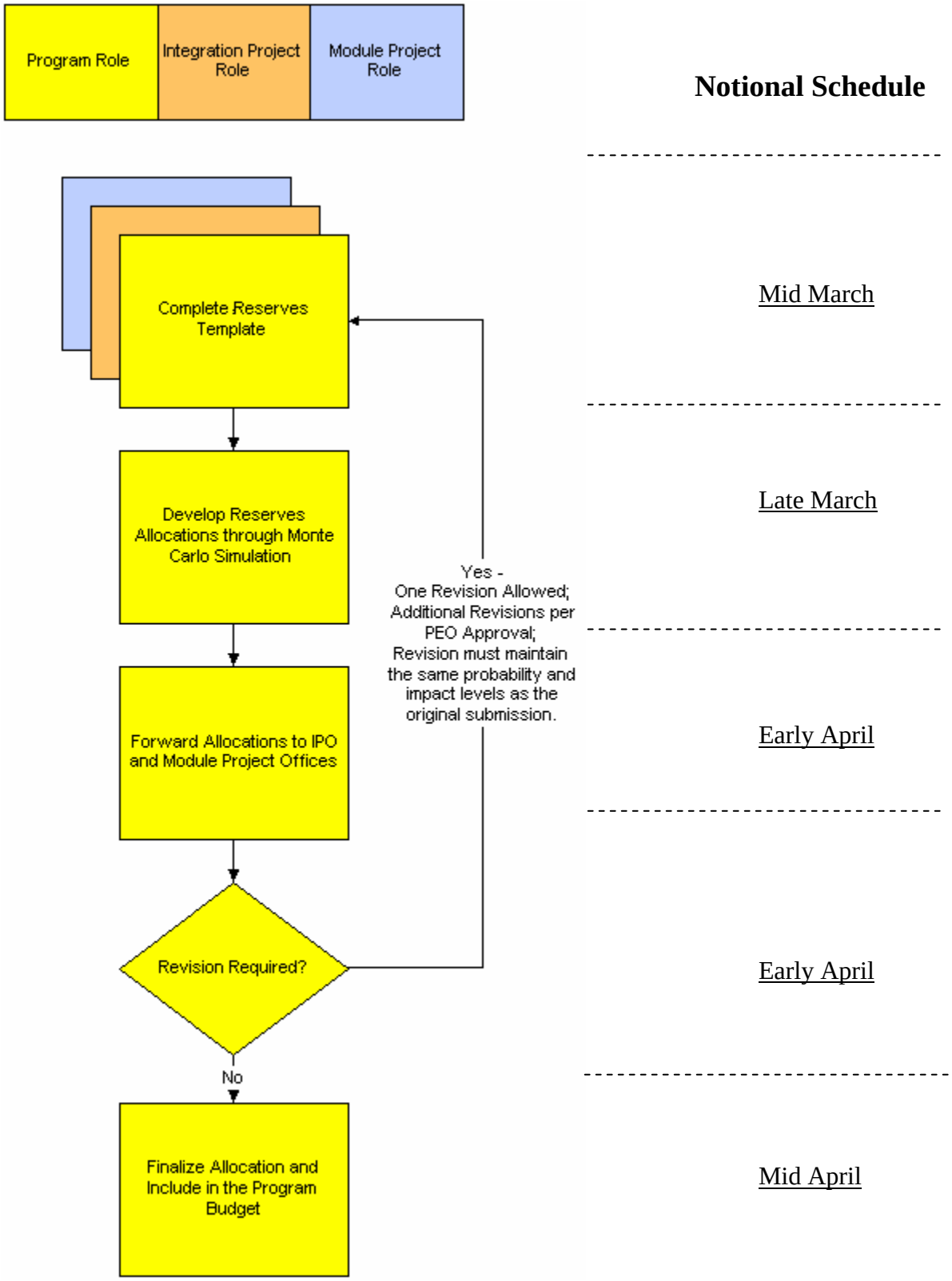
Roles and Responsibilities. The roles and responsibilities for each office are summarized in Table E-1.

Table E-1. Roles and Responsibilities for Contingency Reserves Allocation Process

Roles	Responsibilities
Program Office	▪ Prepare a reserves template. ▪ Use Crystal Ball® to develop Monte Carlo frequency and cumulative distributions for each risk of every submission. ▪ Send analysis of reserves to respective offices for their review and revision. ▪ Review adjusted reserves allocations and approve.
Integration Project Office, Module Project Offices	▪ Complete Program-provided reserves template. ▪ Review reserves allocations and revise, if necessary.

Reserves Process. The flowchart in Figure E-1 illustrates the process as well as a notional timeline of when the respective activities should be accomplished.

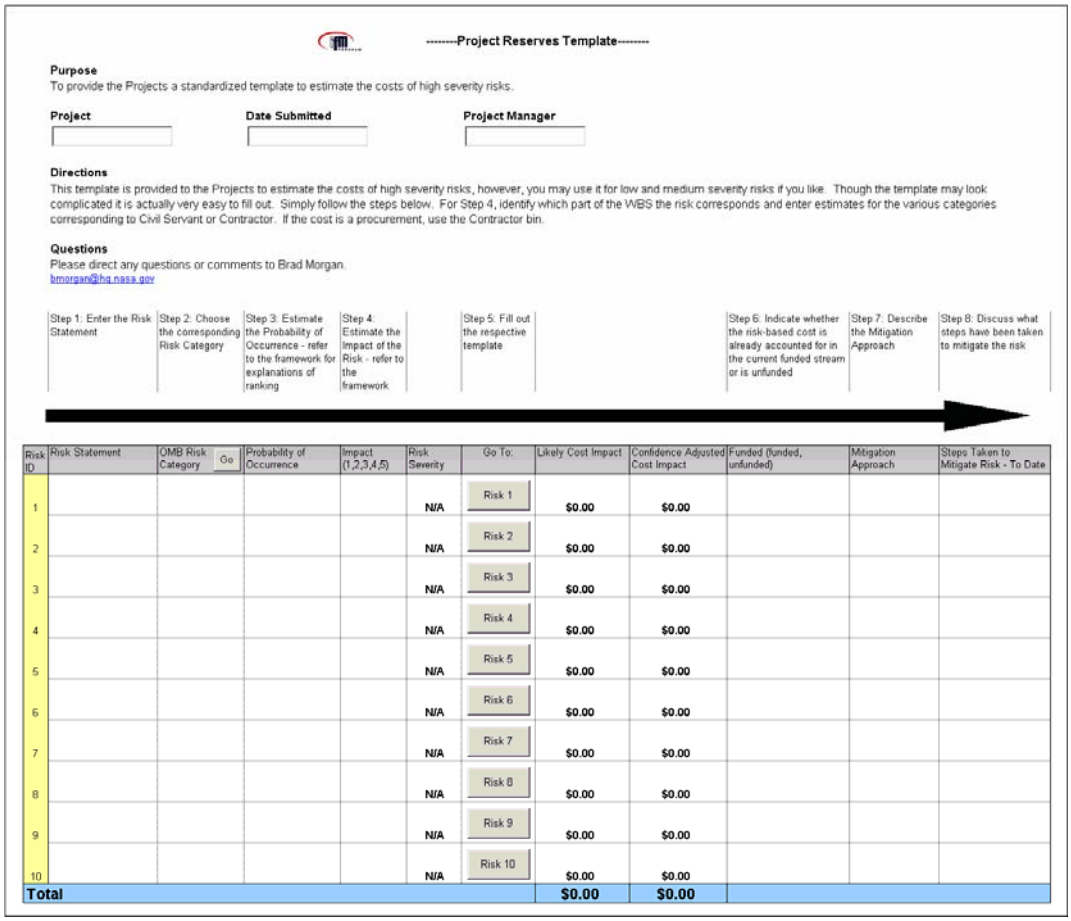
Figure E-1. Contingency Reserves Allocation Process



To complete the reserves template follow the eight steps below, which are also summarized in the Project Reserves Template in Figure E-2.

1. Identify all relevant risks and provide a detailed risk statement.
2. Identify the relevant OMB Risk Categories.
3. Using the Risk Analysis process outlined in this framework, select a Likelihood of Occurrence ranking (1-5). Assign a confidence level according to your selection. (See below for further explanation.)
4. Using the Risk Analysis process outlined in this framework, select a Consequence ranking (1-5).
5. Using the 'Project Reserves Template,' input level of effort (LOE), full-time equivalents (FTE), travel requirements, and software and hardware assumptions that reflect the costs of contingency for the risk, whereby:
    a. Min, Likely, and Max assumptions are required for all assumptions
    b. The assumptions are organized by WBS.
6. Identify whether the reserve is already included in the reserves budget or is not currently funded.
7. Describe the contingency approach – this should reflect the cost assumptions that were made.
8. Describe contingency and/or mitigation steps taken to date for the risk.

Figure E-2. Project Reserves Template



--------Project Reserves Template--------

Purpose
To provide the Projects a standardized template to estimate the costs of high severity risks.

Project | **Date Submitted** | **Project Manager**

Directions
This template is provided to the Projects to estimate the costs of high severity risks, however, you may use it for low and medium severity risks if you like. Though the template may look complicated it is actually very easy to fill out. Simply follow the steps below. For Step 4, identify which part of the WBS the risk corresponds and enter estimates for the various categories corresponding to Civil Servant or Contractor. If the cost is a procurement, use the Contractor bin.

Questions
Please direct any questions or comments to Brad Morgan.
bmorgan@hq.nasa.gov

Step 1: Enter the Risk Statement	Step 2: Choose the corresponding Risk Category	Step 3: Estimate the Probability of Occurrence - refer to the framework for explanations of ranking	Step 4: Estimate the Impact of the Risk - refer to the framework	Step 5: Fill out the respective template	Step 6: Indicate whether the risk-based cost is already accounted for in the current funded stream or is unfunded	Step 7: Describe the Mitigation Approach	Step 8: Discuss what steps have been taken to mitigate the risk

Risk ID	Risk Statement	OMB Risk Category (Go)	Probability of Occurrence	Impact (1,2,3,4,5)	Risk Severity	Go To:	Likely Cost Impact	Confidence Adjusted Cost Impact	Funded (funded, unfunded)	Mitigation Approach	Steps Taken to Mitigate Risk - To Date
1					N/A	Risk 1	$0.00	$0.00			
2					N/A	Risk 2	$0.00	$0.00			
3					N/A	Risk 3	$0.00	$0.00			
4					N/A	Risk 4	$0.00	$0.00			
5					N/A	Risk 5	$0.00	$0.00			
6					N/A	Risk 6	$0.00	$0.00			
7					N/A	Risk 7	$0.00	$0.00			
8					N/A	Risk 8	$0.00	$0.00			
9					N/A	Risk 9	$0.00	$0.00			
10					N/A	Risk 10	$0.00	$0.00			
Total							**$0.00**	**$0.00**			

Contingency Determination and Reserve Allocation. Upon receipt of the completed template, the Program Office will run Monte Carlo simulations to establish a frequency distribution of the cost impacts. Based on the risk likelihood, each risk will be evaluated at a certain confidence level establishing the associated reserve allocation. Confidence levels will be evaluated according to information provided in the template by the Projects. For example, the template requests that the Project provide a likelihood of occurrence based on the following available rankings and associated confidence levels:

Likelihood of Occurrence Ranking	Confidence Level Range
Very Low	1% - 20%
Low	21% - 40%
Moderate	41% - 60%
High	61% - 80%
Very High	81% - 100%

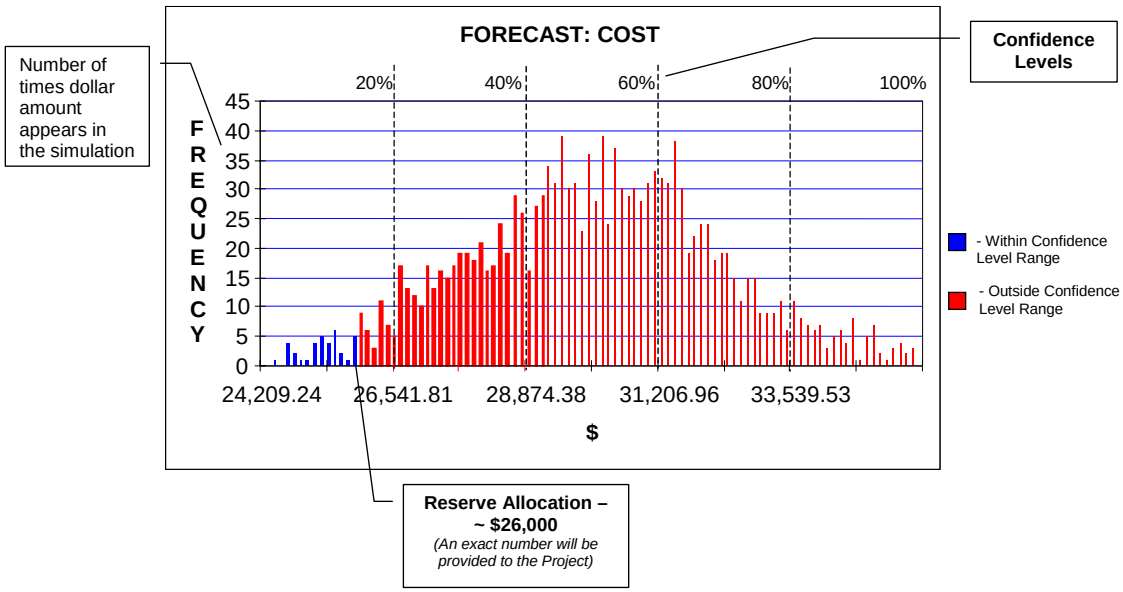
The user is thus asked to choose a likelihood rating and approximate a percentage of confidence that the risk will occur. If a Project selects a likelihood of Very Low and, based on evidence asserts that there is little chance that the risk will actually occur, it can assign a confidence level of 5%. Likewise, if the Project feels that the likelihood is higher, they can assign a confidence level of 20%. This enables the Program to assign a quantifiable measurement to each likelihood rating based on risk knowledge from the Program. If this information is not provided, confidence levels could be assigned too conservatively or to liberally. The Program then runs the risk of allocating too little funding or excessive funding.

If a Project is unsure of the confidence level or does not provide this information in the template, the Program Budget staff will work with the Program Risk Manager to quantify risk likelihood, if possible, or default to the mid-percentage for each Confidence Level Range (i.e., 10% for Very Low, 30% for Low, 50% for Moderate, etc.).

The Program executes the Monte Carlo simulations for each risk. Resulting reserve allocations for each risk are summed to yield the total risk reserve allocation the Project. The Confidence Level outputs and resulting contingency reserve allocations will be sent to each respective Project Office for review (in accordance with the process outlined in Figure E-1. An example of the Confidence Level output for a Very Low Likelihood Rating (Rating = 1) and Confidence Level of 20% is shown in Figure E-3.

Figure E-3. Example – Very Low Confidence Level

Very Low Likelihood of Occurrence
1%-20%



APPENDIX F – RISK COMMUNICATIONS AND REPORTING

The following guidelines, listed in Table F-1, should be used to facilitate Program and Project Risk Communications and Reporting:

Table F-1. Risk Communications and Reporting

Information Sources	Information Provided	Information Recipients	Frequency of Exchange
Independent Reviews/Assessments	• Identified risks • Informed advice	• IFM Program Office • IPO • Module Projects	As identified
Testbed Simulation	Potential software and integration problems	• IPO • Module Projects	As identified
Risk Identification Tools (FTA, FMCEA, Lessons Learned)	Potential risks	• IFM Program Office • IPO • Module Projects • NASA Centers	As identified
• IFM Program Office • IPO • Module Projects • NASA Centers	Risk Status	• IFM Steering Committee • PMC • IAR • Management	Periodic Meeting (according to existing schedules)
IFM Program Office	• Agreements • Guidance • Decisions	• IFM Program Office • IPO • Module Projects • NASA Centers	As required
• IPO • Module Projects • NASA Centers	Top 5 Project Risks and Mitigation Strategies	IFM Program Office	Monthly (via MSR briefing)

LIST OF ACRONYMS

CRMM	Continuous Risk Management Model
COTS	Commercial Off-the-Shelf
eGov	Electronic Government
EOY	End of Year
FMCEA	Failure Mode, Cause, and Effect Analysis
FTA	Fault Tree Analysis
FTE	Full-time Equivalent
IAR	Independent Annual Review
IFM	Integrated Financial Management
IFMP	Integrated Financial Management Program
IPO	Integration Project Office
IT	Information Technology
KSS	Knowledge Sharing System
LLIS	Lessons Learned Information System
LOE	Level of Effort
MSR	Monthly Status Review
NAR	Non-Advocate Review
NASA	National Aeronautics and Space Administration
NPG	NASA Procedures and Guidelines
NPR	NASA Procedural Requirements
OMB	Office of Management and Budget
PMC	Program Management Council
QRR	Quarterly Risk Review
WBS	Work Breakdown Structure